NEW CRITICAL VULNERABILITY ADVISORY: CVE-2026-68579

Summary

CVE-2026-68579 is a newly disclosed Critical vulnerability. It is not yet on CISA's actively-exploited list; treat it as proactive patching before it is weaponised. FreeRDP before 3.30.0 (<= 3.29.0) contains a heap-based buffer overflow in the Windows clipboard client's CliprdrStream_Read function (client/Windows/wf_cliprdr.c). When an OLE paste consumer (e.g. explorer.exe) calls IStream::Read with a fixed-size buffer of cb bytes, CliprdrStream_Read requests file contents from the RDP server and then copies the response into the caller's buffer using the server-supplied length (req_fsize) instead of cb. A malicious or compromised RDP server can return an oversized CB_FILECONTENTS_RESPONSE, causing an out-of-bounds write of attacker-controlled data into the paste consumer's heap buffer when a user pastes server-offered clipboard file contents.

What we know

- **CVE:** CVE-2026-68579
- **Status:** Newly disclosed, not yet known-exploited (not on CISA KEV)
- **Severity:** CVSS 9.6 Critical, Network-exploitable, no privileges required (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:H/A:H)

Recommended action

Patch as a fix becomes available, prioritised by the exposure and EPSS above. Until then, restrict network access to the affected service now (segment it, put it behind a VPN, or take it offline) until you can patch. This does not yet trigger CRA 24-hour reporting, which requires active exploitation, but patching ahead of exploitation is the whole point.

Sources: NIST NVD. Public data; an advisory of a newly disclosed vulnerability, not an incident report. Verify applicability to your estate before acting.